How to securely access Microsoft Azure with Parallels Browser Isolation?

- Parallels Browser Isolation

What is Parallels Browser Isolation (PBI)? :

Learn more about Parallels Browser Isolation!

Why would you like to set up secure access to Microsoft Azure with Parallels Browser Isolation (PBI)?

Like many SaaS applications, users have access to Microsoft Azure from any device and any location by default.

Conditional access in Microsoft Entra Identity (Azure AD) enables you to impose restrictions on managed devices or specific network ranges. However, it's important to understand that these restrictions apply only to managed devices.

What if you want to enforce restrictions without the use of VPN agents? Or suppose you aim to apply access controls to bring-your-own-device (BYOD) policies or non-windows-based devices?

Adding to these challenges, it's crucial to note that conditional access focuses solely on securing entry points. Once access is granted, it does not extend to controlling actions within Microsoft Azure (or any other SaaS application).

What if your security needs include stopping users from downloading data while permitting uploads? Or suppose you need to disable copy/paste functions, prevent screenshot capture, and block printing capabilities? These requirements align with a Zero Trust security model, yet such specific restrictions cannot be achieved through traditional conditional access or role-based access controls alone.

Parallels Browser Isolation enables you to route all Microsoft Azure access through a remote browser. This setup allows for geo-blocking, restricting access exclusively to locations associated with PBI IP addresses.

Following this configuration, only users who adhere to the PBI policies and belong to the designated access groups can connect to Azure. Furthermore, the policy engine empowers you to specify permissible actions within Azure, such as copy/paste, upload, download, print, and others, offering a tailored and secure user experience.

Implement conditional access on Azure

For the first step, you must set up Microsoft Azure to exclusively permit access from PBI IP addresses. You can do this by setting up conditional access within Microsoft Entra ID (formerly known as Azure AD). It's important to highlight that activating this conditional access feature requires a Microsoft Entra Identity P1 license. The process starts with establishing a Named Location encompassing the IP addresses associated with Parallels Browser Isolation.

As an admin, go to “Microsoft Entra ID”, à “Security”, à “Named Locations”

Click on “+ IP ranges location” and give this location a unique name. In my case, I called this location “Parallels Browser Isolation”. Add all IP addresses used by Parallels Browser Isolation. The list can be found online in this KB article: https://kb.parallels.com/en/130095.

When adding the different IP addresses, add a /32 to the end to identify that these are single IPs and not ranges.

Once this is done, go to “Microsoft Entra ID” à “Security” à “Conditional Access”

Click on “+ Create new policy” and give it a unique name. In my case, I called it “PBI Only Policy”.

In configuring the policy, the initial step involves selecting the 'Users' to whom the policy will apply. It's advisable to begin with a small user group for testing purposes before expanding the policy to include a broader audience.

Important: Make sure you exclude at least a few users from this policy, as you might need to get back into your Microsoft Azure if there are configuration or other issues with your conditional access configuration. If you include everyone and you have an issue, you can’t log in to Microsoft Azure anymore and, therefore, can’t make any changes to the conditional access settings in the “Microsoft Entra ID”.

Next, we need to select the “Target Resources” and select “Include”. If you want to protect your Azure portal only, then choose the “Select apps” option and “Select” only “Microsoft Admin Portals”. This application covers access to Microsoft Azure and some other management portals.

Important: If you choose the “All cloud apps” option, take into account that you might have configured your Parallels Browser Isolation (PBI) solution to be federated with “Microsoft Entra ID”, and therefore, you need to

make sure you exclude the application that was created in “Microsoft Entra ID” for PBI from this policy. If not, you won’t be able to log in on PBI.

On the “Conditions” settings, we now have to enable the “Locations” filter. We want this policy enabled for all locations except for the “Parallels Browser Isolation” location created in the first step of this procedure.

To do this, under “Include”, select “Any Network”, and under “Exclude”, select “Select Locations”, and select the “Named Location” you created earlier, in my case “Parallels Browser Isolation” location.

The other conditions like “User risk”, “Sign-in risk”, “Device platforms”, “Client apps”, and “Filter for devices” can remain in the default configuration and don’t need to be modified.

The final steps are to set the “Access Controls” to “Block access”, set “Enable policy” to “On”, and save it.

Publish Microsoft Azure as a Secure Web Application in Parallels Browser Isolation (PBI)

Now that the conditional access is configured, your next step is to ensure the users can access Microsoft Azure via Parallels Browser Isolation (PBI). To do this log in and go to the PBI admin portal. Click on “Applications” -> “Add Application” -> “Secure Web Application”.

Start by setting the “Name“and the “Icon”. Set “https://portal.azure.com” as a start URL.

Under “Domains” you have now to specify all URLs that Azure uses.

For some SaaS applications, this is a single domain, but for Microsoft Azure, the list is pretty long (this is the full list of all domain names used by Microsoft Azure).

You can add the individual subdomains or only the main domains. In the example below we simplified the list of domains to include only the main domains, not the individual subdomains. Also, we added all possible domains, not just the ones linked to the Microsoft Azure login but all the individual services.

The following domains have been added:

aadrm.com	login.live.com	
azconfig.io	microsoft.com	msftauthimages.net
azure.com	microsoftonline-p.com	office.com
azure.net	microsoftonline.com	status.microsoft
azureedge.net	msauth.net	trafficmanager.net
azuresynapse.net	msauthimages.net	windows.net
loganalytics.io	msftauth.net	

Under the “Access for secure web applications” select the users or groups in PBI that must have access to Microsoft Azure.

Optionally, select an extra policy you want to apply to this application. If the policy doesn't exist yet, you must first save the application, create a new policy, and then edit the app and assign the newly created policy.

Before creating the policy, don't forget to save the configuration. You do this by clicking on the bottom of the screen on "Add". Once that is done you will see the app in the list of published apps.

In this example, I want extra security on top of Microsoft Azure. It will create an extra policy to block "copy/paste", "download", and "printing" and have a watermark on the screen to make it more difficult for taking screenshots.

To create a new policy in the right menu bar, click on "Policies" à "Add"

Again, we start with setting a "Name". My policy will be called "Microsoft Apps Policy", and the idea is that I can apply this same policy to other published Microsoft applications I may want to publish in PBI later.

I want to apply the policy to all users, so I will set the filter for "Users and Groups" to disabled.

Same for the "Active Hours", I keep it disabled.

For the "Location," I can implement the geo-restriction. As we have restricted access to Azure to only PBIIP addresses with conditional access, we can't set country-based geo-restrictions at that level. In my example, I have geo-restricted Microsoft Azure access to "Belgium", "France", "Germany", "Italy", "Netherlands", "Portugal" and "Spain".

On the "Security controls/Policy Features", I enabled the "Disable printing", "Disabled downloads", and "Disable Clipboard" features.

Under "Security controls/End-user experience", I enabled the following features:

- "Blue border": This will indicate (blue border around the screen) that you are not accessing the website directly but via the Parallels Browser Isolation solution.
- "Watermarking": This will add the user's login name and date as a watermark on top of the screen so that taking screenshots becomes more difficult.

The "Restrict URLs" options don't need to change here — they can stay on the default values.

Finish creating the policy by clicking on "Save". Now that the policy has been created go back to the "Azure Portal" application and add the "Microsoft Apps Policy" to the application.]

Test the setup

Now that we have published the “Azure Portal” application on PBI and configured the conditional access on Microsoft Entra ID, we can test if the setup works:

First, we try to open it directly from the web browser. This should not work as conditional access only allows connections from the Parallels Brower Isolation IP addresses.

If we do the same thing but via Parallels Browser Isolation, it works. Also, note the watermark and the blue bar around the screen.

Now you have secured access to Microsoft Azure via Parallels Browser Isolation!

Learn more and sign up for Parallels Browser Isolation.
